PATENT
Attorney Docket No. 02100.0066-00

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	)	
	)	
Brett B. BONNER et al.	)	Group Art Unit: 2635
	)	
Application No.: 09/836,350	)	Examiner: Kimberly Y. Jenkins
	)	
Filed: April 18, 2001	)	
	)	
For: SYSTEM AND METHOD FOR CONTROLLING ACCESS TO DESIGNATED AREA	)	Confirmation No.: 8729

Attention: Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

APPEAL BRIEF UNDER BOARD RULE § 41.37

In support of the Notice of Appeal filed February 8, 2006, and further to Board Rule 41.37, Appellants presents this brief and enclose herewith a check for the fee of $500.00 required under 37 C.F.R. § 1.17(c). This Appeal Brief is being filed concurrently with a petition for an Extension of Time for one month, and the appropriate fee. This Appeal responds to the Final Office Action mailed September 8, 2005, which finally rejected claims 1-28.

If any additional fees are required or if the enclosed payment is insufficient, Appellants requests that the required fees be charged to Deposit Account No. 06-0916.

05/09/2006 SZEWDIE1 00000040 09836350
01 FC:1402 500.00 OP
02 FC:1251 120.00 OP

Table of Contents

I. Real Party In Interest

The real party in interest is FedEx Corporation, the assignee of record.

II. Related Appeals and Interferences

There are currently no other appeals or interferences, of which appellants, appellants' legal representative, or assignee are aware, that will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

III. Status Of Claims

In the Advisory Action mailed January 10, 2006 the Examiner maintained the rejection of claims 1-3, 12, and 20 under 35 U.S.C. 102(b) as being anticipated by U.S. Patent No. 5,670,940 to Holcomb et al., the rejection of claims 4, 9, 14, and 21-22 under 35 U.S.C. 103(a) as being unpatentable over Holcomb et al. in view of U.S. Patent No. 6,367,011 to Lee et al., the rejection of claim 13 under 103(a) as being unpatentable over Holcomb et al. in view of U.S. Patent No. 6,484,260 to Scott et al., and the rejection of claims 5-8, 10, 11, 15-19, and 23-28 under 103(a) as being unpatentable over Holcomb et al. in view of Lee et al., in further view of U.S. Patent No. 5,774,053 to Porter.

The final rejections of claims 1-28 are being appealed, and a list of the claims on appeal is found in the attached Claims Appendix.

IV. Status Of Amendments

All claim amendments have been entered.

V. Summary Of Claimed Subject Matter

A. Claims 1 and 20

Independent claim 1 recites a system for controlling access to a designated area, the designated area having a security device to control access. The system includes a programmable unit to generate a first and second key for each access to the designated area. The system also includes a programming unit to generate an access key using the first key and a programmable tag to store the access key. The system also includes a validation system including a control unit to generate a validation key using the second key, a memory to store the validation key, and a communication device to establish a data communication with the programmable tag to receive the access key. The control unit compares the access key and the validation key and causes the security device to allow access to the designated area if the access key matches the validation key. The subject matter of claim 1 is described in the specification at least at page 5, line 21 through page 13, line 21 and FIGs 2 and 3.

Independent claim 20 recites a method for controlling access to a designated area, the designated area having a security device to control access. The method comprises generating a first and second key for each access to the designated area. The method also comprises using the first key, generating an access key and using the second key, generating a validation key. The method also comprises comparing the access key and the validation key and causing the security device to allow access to the designated area, if the access key matches the validation key. The subject matter of claim 1 is described in the specification at least at page 5, line 21 through page 13, line 21 and FIGs. 2 and 3.

B. Claims 2 - 7

The subject matter set forth in claim 2 relates to a method, as set forth in claim 1, wherein the programmable unit and the programming unit are integrated in a single unit. The subject matter of claim 2 is described in the specification at least at page 6, lines 3-4.

The subject matter set forth in claim 3 relates to a method, as set forth in claim 1, wherein the control unit is a microprocessor. The subject matter of claim 3 is described in the specification at least at page 6, line 19.

The subject matter set forth in claim 4 relates to a method, as set forth in claim 1, wherein the memory is a nonvolatile memory. The subject matter of claim 4 is described in the specification at least at page 6, line 21.

The subject matter set forth in claim 5 relates to a method, as set forth in claim 1, wherein the communication device includes a transceiver to establish a wireless data communication with a corresponding transceiver included in the programmable tag. The subject matter of claim 5 is described in the specification at least at page 7, lines 7-11.

The subject matter set forth in claim 6 relates to a method, as set forth in claim 1, wherein the transceivers are radio frequency transceivers. The subject matter of claim 6 is described in the specification at least at page 7, lines 7-11.

The subject matter set forth in claim 7 relates to a method, as set forth in claim 1, wherein the validation system includes an antenna for transmitting and receiving radio frequency signals. The subject matter of claim 7 is described in the specification at least at page 7, lines 7-11.

C. Claim 8

The subject matter set forth in claim 8 relates to a method, as set forth in claim 1, wherein the validation system further includes a proximity detector causing the communication device to initiate the wireless data communication with the programmable tag upon detecting an object outside the designated area. The subject matter of claim 8 is described in the specification at least at page 7, lines 11-20.

D. Claim 9

The subject matter set forth in claim 9 relates to a method, as set forth in claim 1, wherein the communication device is a programmable tag reader exposed outside the designated area to establish a wired data communication with the programmable tag. The subject matter of claim 9 is described in the specification at least at page 12, lines 7-11.

E. Claims 10 - 11

The subject matter set forth in claim 10 relates to a method, as set forth in claim 1, wherein the validation system includes an input device to enter the second key. The subject matter of claim 10 is described in the specification at least at page 6, line 6.

The subject matter set forth in claim 11 relates to a method, as set forth in claim 1, wherein the input device is a keypad. The subject matter of claim 11 is described in the specification at least at page 6, lines 20-21.

F. Claim 12 and 13

The subject matter set forth in claim 12 relates to a method, as set forth in claim 1, wherein the security device is an electronic lock. The subject matter of claim 12 is described in the specification at least at page 5, lines 11-14.

The subject matter set forth in claim 13 relates to a method, as set forth in claim 1, wherein the security device is a garage door opener. The subject matter of claim 13 is described in the specification at least at page 5, lines 11-14.

G. Claim 14

The subject matter set forth in claim 14 relates to a method, as set forth in claim 1, wherein, for each access to the designated area, the programmable unit randomly generates an encryption key to be included in both the first and second keys. The subject matter of claim 14 is described in the specification at least at page 8, lines 6-17.

H. Claims 15-16 and 26-27

The subject matter set forth in claim 15 relates to a method, as set forth in claim 1, wherein the control unit causes the security device to terminate the access to the designated area after a predetermined period of time. The subject matter of claim 15 is described in the specification at least at page 11, lines 19 through page 12, line 11.

The subject matter set forth in claim 16 relates to a method, as set forth in claim 15, wherein the control unit prevents further access to the designated area after the predetermined period of time. The subject matter of claim 16 is described in the specification at least at page 11, lines 19 through page 12, line 11

The subject matter set forth in claim 26 relates to a method, as set forth in claim 20, further comprising the step of causing the security device to terminate the access to the designated area after a predetermined period of time. The subject matter of claim 26 is described in the specification at least at page 11, lines 19 through page 12, line 11.

The subject matter set forth in claim 27 relates to a method, as set forth in claim 26, further comprising the step of preventing further access to the designated area after the predetermined period of time. The subject matter of claim 27 is described in the specification at least at page 11, lines 19 through page 12, line 11.

I. Claims 17-19 and 28

The subject matter set forth in claim 17 relates to a method, as set forth in claim 1, wherein the control unit includes a clock to determine the time and date of the access. The subject matter of claim 17 is described in the specification at least at page 6, lines 18-20.

The subject matter set forth in claim 18 relates to a method, as set forth in claim 17, wherein the control unit stores the time and date of the access in the memory. The subject matter of claim 18 is described in the specification at least at page 6, lines 18-20.

The subject matter set forth in claim 19 relates to a method, as set forth in claim 17, wherein the communication device transmits to and stores in the programmable tag the time and date of the access. The subject matter of claim 19 is described in the specification at least at page 12, lines 3-5.

The subject matter set forth in claim 28 relates to a method, as set forth in claim 20, further comprising the step of storing the time and date of the access. The subject matter of claim 28 is described in the specification at least at page 12, lines 3-5.

J. Claims 21-25

The subject matter set forth in claim 21 relates to a method, as set forth in claim 20, wherein the first key generating step comprises the steps of randomly generating an

encryption key; and combining the encryption key with a third key. The subject matter of claim 21 is described in the specification at least at page 8, line 18 through page 9, line 17.

The subject matter set forth in claim 22 relates to a method, as set forth in claim 21, wherein the second key generating step comprises the step of combining the encryption key with a fourth key. The subject matter of claim 22 is described in the specification at least at page 9, line 18 through page 10, line 16.

The subject matter set forth in claim 23 relates to a method, as set forth in claim 22, wherein the third key is the address of the designated area and the fourth key is an agent code. The subject matter of claim 23 is described in the specification at least at page 8, line 18 through page 10, line 16.

The subject matter set forth in claim 24 relates to a method, as set forth in claim 23, wherein the access key generating step comprises the steps of entering the first key, the agent code, the address, and an access date; comparing the entered address and the address in the first key; and using the encryption key, encrypting the agent code, the access date, and the address if the entered address matches the address in the first key. The subject matter of claim 24 is described in the specification at least at page 8, line 18 through page 10, line 16.

The subject matter set forth in claim 25 relates to a method, as set forth in claim 24, wherein the validation key generating step comprises the steps of entering the second key, the agent code, the address, and the access date; comparing the entered agent code and the agent code in the second key; and; using the encryption key, encrypting the agent code, the access date, and the address if the entered agent code

matches the agent code in the second key. The subject matter of claim 25 is described in the specification at least at page 8, line 18 through page 10, line 16.

K. Overview

The inventions at issue are defined by the claims, each of which represent a separate invention, without in any manner limiting the full scope of the claims, Appellants will generally overview certain aspects of the invention, to assist the Board in its consideration of and decision on the issues before it.

Generally, the invention is directed to a programmable system that generates an agent key and a customer key for each access to an area. The agent that will access the designated area receives the agent key and the customer authorizing an unattended access to a designated area receives the customer key. The programmable unit randomly generates an encryption key for each access to the area and generates the agent key by combining the encryption key with a piece of information about the area. The programmable unit generates the customer key by combining the same encryption key with a piece of information about the agent. (See specification, page 6-17).

The agent also enters the agent key, its agent code, the access date, and the address into a programming unit which first performs an internal validation and then generates an encrypted access key and stores the encrypted key in a programmable tag. (See specification, page 8: line 18-page 9: line 18). The customer also enters the customer key, agent code, address of the area, and the access date into the validation system. After the customer enters this information, a control unit performs an internal validation before generating a validation key. If the agent code in the customer key and the separately entered agent code as entered by the customer match, the control unit

generates and encrypted validation key. (See specification, page 9: line 18-page 10: line 16).

On the access date, the control unit activates a proximity sensor to monitor a limited area outside of the customer's designated area for an object. (See specification, page 10: 17-20). When the proximity detector senses an object, the control unit causes the communication device to begin transmitting signals. The programmable tag may be carried by the agent and the tag detects the signals transmitted from the communication device and responds by transmitting the encrypted access key stored therein. (See specification, page 10: line 21 - page 11: line 10). The communication device receives the encrypted access key and other access information transmitted by the programmable tag and sends them to the control unit. The control unit compares the encrypted access key with the encrypted validation key stored in its memory for the current date. If the encrypted access key matches the encrypted validation key, control unit activates the a security device to allow the agent's employee access to the designated area. (See specification, page 11: lines 11-19).

VI. Grounds of Rejection

A. Claims 1-3, 12, and 20 stand rejected under 35 U.S.C. 102(b) as being anticipated by U.S. Patent No. 5,670,940 to Holcomb et al.

B. Claims 4, 9, 14, and 21-22 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Holcomb et al. in view of U.S. Patent No. 6,367,011 to Lee et al.

C. Claim 13 stands rejected under 103(a) as being unpatentable over Holcomb et al. in view of U.S. Patent No. 6,484,260 to Scott et al.

D. Claims 5-8, 10, 11, 15-19, and 23-28 remain rejected under 103(a) as being unpatentable over Holcomb et al. in view of Lee et al., in further view of U.S. Patent No. 5,774,053 to Porter.

VII. Argument

Each claim of this patent application is separately patentable, and upon issuance of a patent will be entitled to a separate presumption of validity under 35 U.S.C. § 282. The grounds for rejection and Appellants' responses raise a number of distinct and independent uses. Therefore, all of the claims do not stand or fall together.

A. The Board Should Reverse the Rejection of Claims 1-3, 12, and 20 Under § 102(e) Because the Applied Reference Does Not Anticipate the Claims

Appellants respectfully submit that the Examiner's rejection of claims 1-3 and 12 should be reversed. To properly anticipate Appellants' claimed inventions, the Examiner must demonstrate that each and every element of the claims in issue are either expressly described or necessarily inherent in a single prior art reference. See Perkin-Elmer Corp. v. Computervision Corp., 732 F.2d 888, 894, 221 U.S.P.Q. 669, 673 (Fed. Cir. 1984). Furthermore, "[t]he identical invention must be shown in as complete detail as is contained in the . . . claim." See M.P.E.P. § 2131, quoting Richardson v. Suzuki Motor Co., 868 F.2d 1126, 1236, 9 U.S.P.Q.2d 1913, 1920 (Fed. Cir. 1989). In addition, "[t]he elements must be arranged as required by the claim." M.P.E.P. § 2131.

Because the Examiner relies upon Holcomb et al. as the principal reference in all of his rejections, Appellants will discuss that reference in some detail. Holcomb et al. is directed to a system that operates to block access to a room when a key has been used and the guest is detected as being present in the room. (Abstract.) The blocking function of the lock is initiated or turned on each time a guest key card is inserted into the lock and the guest enters the room. (Col. 2, ll. 15-19.) The key card that is inserted

into the lock contains a key code and if that matches an access code, the door opens. (Col. 4, ll. 40-44.)

Holcomb et al. further describes that its electronic lock systems comprise a key-generating station as well as an electronic lock, which is mounted in a door of a room that provides access to the room. (Col. 1, ll. 16-20.) The lock has a means to read the magnetic data (key code) on the key, and the microcontroller on the lock compares the key code with an access code. (Col. 1, ll. 26-28.) The "access code is either generated by the microcontroller through an algorithm or is stored in the memory of the microcontroller." (Col 1, ll. 28-31.) In order to ensure that the access code and the key code match, three possible situations are possible: (1) the key-generating station is either hard wired to the electronic lock so it can communicate the new key code to the electronic lock (where the access code is generated); (2) the key-generating station and the microcontroller use the same algorithm to calculate the codes; or (3) the key-generating station and the microcontroller store the same codes. (Col. 1, ll. 36-38.)

Independent claim 1 recites, inter alia:

> a programmable unit to generate a first and second key for each access to the designated area;
> a programming unit to generate an access key using the first key;
> a programmable tag to store the access key; and
> a validation system including a control unit to generate a validation key using the second key, ...

In the Office Action, the Examiner alleges that Holcomb et al. discloses "a programmable unit (key-generating station) . . . which generates a first key, which is the signal that causes the algorithm used within the programmable unit (key-generating station) to generate the access key that is programmed to the tag." The Examiner also

alleges that Holcomb et al. teaches that "[t]he programmable unit (key-generating station) communicates the second key to the validation unit (electronic lock) by transmitting a signal (second key) to an algorithm for the microcontroller of the lock (Col. 1, ll. 26-28, 26-38) to create a key, which is the validation key that is stored and later compared to the access key of the tag." (Office Action, p. 2.) Appellants disagree.

First, contrary to the Examiner's assertions, there is no disclosure or teaching of a "signal that causes the algorithm used . . . to generate the access key" (id.) in Holcomb et al. Should the Examiner maintain the rejection after considering the arguments presented herein, Appellants submit that the Examiner must provide "the explicit basis on which the examiner regards the matter as subject to official notice and [allow Appellants] to challenge the assertion in the next reply after the Office Action in which the common knowledge statement was made" (Memo. p. 3 (emphasis in original)), or else reverse the rejection of independent claims 1 and 12.

Second, the cited portions of Holcomb et al. state that a microcontroller is stored on an electronic lock, and "the access code [i.e., the alleged validation key] is either generated by the microcontroller through an algorithm or is stored in the memory of the microcontroller." (Col. 1, ll. 26-28.) Therefore, contrary to the Examiner's assertion, Holcomb et al. does not "generate a validation key using the second key," as recited in claim 1. Rather, the system disclosed by Holcomb et al. merely creates an access key [the alleged validation key] through an algorithm or retrieves an access key **already stored** in microcontroller 13. Holcomb et al. provides no teaching of generating a validation key based upon a second key.

Finally, the algorithm mentioned in Holcomb et al. cannot be a teaching of the "first key" and "second key" of claim 1 because Holcomb et al. specifically states that "the microcontroller use[s] the **same algorithm** to calculate the codes," referring to the key code and access code. (Col. 1, ll. 37-38) (emphasis added). Claim 1, however, recites that the "access key [is generated] using the first key," while the "validation key [is generated] using the second key." At most Holcomb et al. teaches using the same algorithm to generate the key code and the access code, which is not a teaching or suggestion of "a programming unit to generate an access key using the first key . . . and a validation system including a control unit to generate a validation key using the second key," as recited in claim 1.

Since Holcomb et al. fails to teach at least the above-quoted element of claim 1, Holcomb et al. cannot anticipate independent claim 1. Independent claim 20 recites similar limitations, for example, "using the second key, generating a validation key." Holcomb et al. thus also fails to anticipate claim 20 for at least the reasons given above with respect to claim 1. Therefore, Appellants respectfully request the rejection of claims 1 and 20 under 35 U.S.C. § 102(b) be reversed and the claims allowed.

Claim 3 depends from claim 1. Accordingly, the cited art does not support the rejection of dependent claim 3 for at least the same reasons as set forth above in connection with claim 1. Therefore, Appellants request that the rejection of these claims be reversed and the claims allowed.

B. The Board Should Reverse the Rejection of Claims 4, 9, and 14 Under § 103(a) Because a Prima Facie Case of Obviousness Has Not Been Established

Appellants further respectfully submit that the Examiner's rejection of claims 4, 9, and 14 under 35 U.S.C. § 103(a) should be reversed. Several basic factual inquiries must be made in order to determine the obviousness or nonobviousness of claims of a patent application under 35 U.S.C. § 103. These factual inquiries, set forth in Graham v. John Deere Co., 383 U.S. 1, 17, 148 U.S.P.Q. 459, 467 (1966), require the Examiner to:

> (1) determine the scope and content of the prior art;
> (2) ascertain the differences between the prior art and the claims in issue;
> (3) resolve the level of ordinary skill in the pertinent art; and
> (4) evaluate evidence of secondary considerations.

The obviousness or nonobviousness of the claimed invention is then evaluated in view of the results of these inquiries. Id., 383 U.S. at 17-18, 148 U.S.P.Q. at 467.

In order to carry the initial burden of establishing a prima facie case of obviousness that satisfies the Graham standard, the Examiner must show that the cited prior art references teach or suggest all the claim limitations. In re Royka, 490 F.2d 981, 180 U.S.P.Q. 580 (C.C.P.A. 1974). The Examiner must also show that there is some suggestion or motivation, either in the references or in the knowledge generally available to one of ordinary skill in the art, to modify the reference. In re Rouffet, 149 F.3d 1350, 47 U.S.P.Q.2d 1453 (Fed. Cir. 1998). Finally, the Examiner must show that the select teachings could be combined with a reasonable expectation of success. In re Dow Chem., 837 F.2d 469, 473, 5 U.S.P.Q.2d 1529, 1531 (Fed. Cir. 1988). In this

case, the Examiner has not set forth showings sufficient to establish at least two of these requirements.

"The examiner bears the initial burden of factually supporting any prima facie conclusion of obviousness." M.P.E.P. § 2142. In doing so, "all the words in a claim must be considered in judging the patentability of that claim against the prior art." In re Wilson, 424 F.2d 1382, 1385, 165 U.S.P.Q. 494, 496 (C.C.P.A. 1970). Further, the Federal Circuit has opined that "virtually all [inventions] are combinations of old elements." See, e.g., In re Rouffet, 149 F.3d at 1357, 47 U.S.P.Q.2d at 1457 (citations omitted). In fact, the Federal Circuit in Rouffet explained that very often an examiner may find every element of a claimed invention in the prior art, but mere identification is not sufficient to negate patentability. Id. Instead, the court stated that "the examiner must show reasons that the skilled artisan, confronted with the same problems as the inventor and with no knowledge of the claimed invention, would select the elements from the cited prior art references for combination in the manner claimed." Id. As such, evidence to select the specific elements may "flow from the prior art references themselves, the knowledge of one of ordinary skill in the art, or, in some cases, from the nature of the problem to be solved." Pro-Mold & Tool Co. v. Great Lakes Plastics, Inc., 75 F.3d 1568, 1573, 37 U.S.P.Q.2d 1626, 1630 (Fed. Cir. 1996).

As stated above, Holcomb et al. fails to disclose at least "a validation system including a control unit to generate a validation key using the second key," as well as "using the second key, generating a validation key," language that is recited in claims 4, 9, and 14. Nothing in Lee et al. teaches or suggests these limitations, as Lee et al. is cited by the Examiner only for allegedly disclosing a nonvolatile memory, a

programmable tag reader, and multiple encryption keys. Therefore, Lee et al. fails to overcome the deficiencies of Holcomb et al. Accordingly, no prima facie case of obviousness has been established with respect to claims 4, 9, and 14. Appellants respectfully request that the rejection of claims 4, 9, and 14 under 35 U.S.C. § 103(a) be reversed.

C. The Board Should Reverse the Rejection of Claims 21 and 22 Under § 103(a) Because a Prima Facie Case of Obviousness Has Not Been Established

Appellants respectfully submit that the rejection of claims 21 and 22 under 35 U.S.C. § 103(a) as being obvious over Holcomb et al. in view of Lee et al. should be reversed. Claim 21 recites, "randomly generating an encryption key; and combining the encryption key with a third key." Claim 21 depends from claim 20. As discussed above, Holcomb et al. fails to teach or suggest every element of claim 20. Furthermore, Lee et al. does not compensate for the shortcomings of Holcomb et al.

The Examiner alleges that Holcomb et al. discloses "a key-generating station for generating a third and fourth key, which are the access codes to another programmable unit and electronic lock," citing column 1, lines 16-22, of Holcomb et al. The cited portions of Holcomb et al., however, merely describe providing "each new guest with a new key," and the electronic lock system can "re-key the lock for each new key used in the lock." (Col. 1, ll. 16-19.) There is no disclosure of a "third" and "fourth" key, as asserted by the Examiner. Therefore, Holcomb et al. fails to teach or suggest "randomly generating an encryption key; and combining the encryption key with a third key," as recited by claim 21.

Furthermore, the Examiner applies Lee et al., alleging that Lee et al. discloses "the encryption key generating means . . . as aforementioned regarding claim 14." (Office Action, p. 7.) Lee et al., however, describes generating keys based on a single other key, for example, "a master load key (KML) used to create a derived unique load key (KDL)," or "a supplier update key (KMC) used to create a derived unique supplier

update key (KDC)." (Col. 7, ll. 57-64.) Lee et al. also describes encrypting secret data "under a key encryption key when generated." Lee et al. further states that the system "decrypts the secret data, re-encrypts it under a personalization key known to the card and then the encrypted secret data is loaded onto the card using personalization device 150." (Col. 8, ll.21-33.) Therefore, Lee et al. merely describes encryption in general using only one key. There is no motivation to combine the encrypted key in Lee et al. with the alleged third key of Holcomb et al. because Lee et al. describes only using one key for the encryption process. Accordingly, no prima facie case of obviousness has been established with respect to claim 21. Claim 22 is also dependent from claim 21, an allowable claim. Appellants respectfully request that the rejection of claims 21 and 22 under 35 U.S.C. § 103(a) be reversed.

D. The Board Should Reverse the Rejection of Claim 13 Under § 103(a) Because A Prima Facie Case of Obviousness Has Not Been Established

Appellants further respectfully submit that the Examiner's rejection of claim 13 under 35 U.S.C. § 103(a) should be reversed. Claim 13 depends from claim 1. As stated above, Holcomb et al. fails to disclose at least "a validation system including a control unit to generate a validation key using the second key," as recited in claim 1. No disclosure in Scott et al. teaches or suggests these limitations, as Scott et al. is cited by the Examiner only for allegedly disclosing a "garage door opener." Therefore, Scott et al. fails to overcome the deficiencies of Holcomb et al. Accordingly, no prima facie case of obviousness has been established with respect to claim 13. Appellants respectfully request that the rejection of claim 13 under 35 U.S.C. § 103(a) be reversed.

E. The Board Should Reverse the Rejection of Claims 5-7, 10, 11, and 17-19 Under § 103(a) Because a Prima Facie Case of Obviousness Has Not Been Established

Appellants further respectfully submit that the Examiner's rejection of claims 5-7, 10, 11, and 17-19 under 35 U.S.C. § 103(a) should be reversed. Claims 5-7, 10, 11, and 17-19 depend from claim 1. As stated above, Holcomb et al. fails to disclose at least "a validation system including a control unit to generate a validation key using the second key," as recited in claim 1. Nothing in Lee et al. teaches or suggests these limitations, as Lee et al. is cited by the Examiner only for allegedly disclosing a "smart card." Porter also fails to overcome the deficiencies of Holcomb et al. Accordingly, no prima facie case of obviousness has been established with respect to claims 5-7, 10, 11, and 17-19. Appellants respectfully request that the rejection of claims 5-7, 10, 11, and 17-19 under 35 U.S.C. § 103(a) be reversed and the claims allowed.

F. The Board Should Reverse the Rejection of Claim 8 Under § 103(a) Because A Prima Facie Case of Obviousness Has Not Been Established

Appellants respectfully submit that the rejection of claim 8 under 35 U.S.C. § 103(a) as being obvious over Holcomb et al. in view of Lee et al. should be reversed. Claim 8 recites, "wherein the validation system further includes a proximity detector causing the communication device to initiate the wireless data communication with the programmable tag upon detecting an object outside the designated area." (Emphasis added.) Claim 8 depends from claim 1. As discussed above, Holcomb et al. fails to teach or suggest every element of claim 1. Furthermore, Lee et al. does not compensate for the shortcomings of Holcomb et al.

The Examiner applies Lee et al., alleging that Lee et al. discloses "a smart card, which is passive, that may interface with a variety of devices in order to gain access via the wireless communication." The Examiner further states that "it is well known to one skilled in the art to know that a smart card, which is passive, utilizes proximity detection in order for the card to be read by a reader. Therefore, according to the Examiner, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have the proximity detector of Lee et al. into the system of Holcomb et al., because Holcomb et al. teaches a card reader in that which the card is inserted, whereas Lee et al. teaches a passive device." (Final Office Action, p. 10.)

First, none of the disclosure associated with Lee et al. teaches or suggests a "validation system further includes a proximity detector causing the communication device to initiate the wireless data communication with the programmable tag upon

detecting an object outside the designated area," as recited in claim 8. (Emphasis added.) Appellants request that the Examiner's Answer specially identify what specific disclosure of Lee et al. is being relied upon for disclosing the quoted claim language.

Furthermore, Appellants disagree with the Examiner's allegations and conclusions, because they are unsubstantiated statements of questionable relevance to Appellants' claimed invention. Appellants further refer the Examiner to the February 21, 2002 Memorandum from USPTO Deputy Commissioner for Patent Examination Policy, Stephen G. Kunin, regarding "Procedures for Relying on Facts Which are Not of Record as Common Knowledge or for Taking Official Notice." In relevant part, the Memorandum states, "If the examiner is relying on personal knowledge to support the finding of what is known in the art, the examiner must provide an affidavit or declaration setting forth specific factual statements and explanation to support the finding." (Memo. p. 3.) Further, the Memorandum indicates that the Federal Circuit has "criticized the USPTO's reliance on 'basic knowledge' or 'common sense' to support an obviousness rejection, where there was no evidentiary support in the record for such a finding." (Id. at 1.)

Appellants submit that "[d]eficiencies of the cited references cannot be remedied by general conclusions about what is 'basic knowledge' or 'common sense.'" In re Lee, 61 U.S.P.Q.2d 1430, 1432-33 (Fed. Cir. 2002), quoting In re Zurko, 59 U.S.P.Q.2d 1693, 1697 (Fed. Cir. 2001). Should the Examiner maintain the rejection after considering the arguments presented herein, Appellants submit that the Examiner must provide "the explicit basis on which the examiner regards the matter as subject to official notice and [allow Appellants] to challenge the assertion in the next reply after the Office

Action in which the common knowledge statement was made" (Memo. p. 3 (emphasis in original)), or else reverse the rejection of dependent claim 8.

G. The Board Should Reverse the Rejection of Claims 15 and 16 Under § 103(a) Because a Prima Facie Case of Obviousness Has Not Been Established

Appellants respectfully submit that the rejection of claims 15 and 16 under 35 U.S.C. § 103(a) as being obvious over Holcomb et al. in view of Porter should be reversed. Claim 15 recites "wherein the control unit causes the security device to terminate the access to the designated area after a predetermined period of time." (Emphasis Added) Claim 15 depends from claim 1. As discussed above, Holcomb et al. fails to teach or suggest every element of claim 1. Furthermore, Porter does not compensate for the shortcomings of Holcomb et al.

The Examiner applies Porter, alleging that "Porter teaches the control unit causes the security device . . . to terminate the access to the designated area 10 after a predetermined period of time, for the controller 46 may be equipped to an audio indication for security to be programmed to send a message to law enforcement as a means to prevent unauthorized users from tampering with the designated area," citing column 6, lines 54-64, of Porter.

The cited portions of Porter, however, merely describe that a controller "may be programmed to activate the alarm bell if either of the doors 18, 20 of the enclosure 14 are forced open or if a person otherwise tampers with the storage device without first entering a valid vendor code or homeowner code." (Col. 6, ll. 56-63.) Porter is completely silent on any teaching or suggestion of at least "predetermined period of time," much less "wherein the control unit causes the security device to terminate the access to the designated area after a predetermined period of time," as recited in claim

15. For at least these reasons, the references fail to teach or suggest all of the elements of claim 15. Therefore, a prima facie case of obviousness has not been established. Claim 16 also depends from claim 15, and as discussed above, Holcomb et al. and Porter fail to teach or suggest every element of claim 15. Therefore, claim 16 is allowable at least by its dependence from allowable claim 15. Appellants therefore request the Board should reverse the § 103 rejections of these claims.

H. The Board Should Reverse the Rejection of Claims Claim 23-28 Under § 103(a) Because a Prima Facie Case of Obviousness Has Not Been Established

Appellants respectfully submit that the rejection of claims 23-28 under 35 U.S.C. § 103(a) as being obvious over Holcomb et al. in view of Porter should be reversed. Claim 23 recites "wherein the third key is the address of the designated area and the fourth key is an agent code." Claim 23 depends from claim 1. As discussed above, Holcomb et al. fails to teach or suggest every element of claim 1. Furthermore, Porter does not compensate for the shortcomings of Holcomb et al.

Furthermore, the Examiner alleges that Porter "discloses valid 'keys' as being an address (homeowner code) and an agent (vendor) code," citing column 6, lines 56-61. The cited portions of Porter, however, state that a controller may be programmed to activate an alarm if either doors of the enclosure are forced open or if a person otherwise "tampers with the storage device without first entering a valid vendor code or homeowner code." (Col. 6, ll. 56-61.) A homeowner code, however, is not a teaching or suggestion of the claimed "address of the designated area," as recited in claim 23.

Furthermore, claim 23, which depends from claim 21, states in combination "combining the encryption key with a third key, wherein the third key is the address of the designated area and the fourth key is an agent code." The Examiner states with regard to claim 21 that "Lee discloses the encryption key generating means for each programmable unit as aforementioned regarding claim 14." (Final Office Action, p. 7.) The Examiner, however, has no motivation to combine these references. Lee et al. states that "secret data is encrypted under a key encryption key when generated. In a

second embodiment, secret data is encrypted under a personalization encryption key known to the card when the secret data is generated at the issuer location. Device 150 loads this encrypted data to the card **without modification**." (Col. 8: 24-34) (emphasis added). Therefore, there is no motivation in Lee et al. to combine the encrypted key with the "homeowner code" or "vendor code" of Porter because Lee et al. specifically states that the "device 15 loads this encrypted data **without modification**." The encrypted key in Lee et al. is not meant to be modified. For at least these reasons, the references not only fail to teach or suggest all of the elements of claim 23, but there is also no motivation to combine the references. Furthermore, claims 24 and 25 depend from claim 23, an allowable claim, and claims 26-28 depend from claim 20, and as discussed above, Holcomb et al. fails to teach or suggest every element of claim 20. Therefore, a prima facie case of obviousness has not been established and the Board should reverse the § 103 rejections of claims 23-28.

VIII. Conclusion

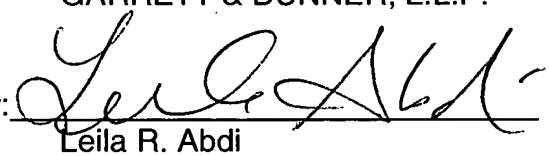
For the reasons given above, pending claims 1-28 are allowable. Therefore, Appellants respectfully request the Board to reverse the Examiner's rejection.

To the extent any extension of time under 37 C.F.R. § 1.136 is required to obtain entry of this Appeal Brief, such extension is hereby respectfully requested. If there are any fees due under 37 C.F.R. §§ 1.16 or 1.17 that are not enclosed herewith, including any fees required for an extension of time under 37 C.F.R. § 1.136, please charge such fees to our Deposit Account No. 06-0916.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

Dated: May 8, 2006

By: 
Leila R. Abdi
Reg. No. 52,399

Claims Appendix to Appeal Brief Under Rule 41.37(c)(1)(viii)

1. (Original) A system for controlling access to a designated area, the designated area having a security device to control access thereto, comprising:

a programmable unit to generate a first and second key for each access to the designated area;

a programming unit to generate an access key using the first key;

a programmable tag to store the access key; and

a validation system including a control unit to generate a validation key using the second key, a memory to store the validation key, and a communication device to establish a data communication with the programmable tag to receive the access key therefrom, the control unit comparing the access key and the validation key and causing the security device to allow access to the designated area if the access key matches the validation key.

2. (Original) The system of claim 1, wherein the programmable unit and the programming unit are integrated in a single unit.

3. (Original) The system of claim 1, wherein the control unit is a microprocessor.

4. (Original) The system of claim 1, wherein the memory is a nonvolatile memory.

5. (Original) The system of claim 1, wherein the communication device includes a transceiver to establish a wireless data communication with a corresponding transceiver included in the programmable tag.

6. (Original) The system of claim 5, wherein the transceivers are radio frequency transceivers.

7. (Original) The system of claim 6, wherein the validation system includes an antenna for transmitting and receiving radio frequency signals.

8. (Original) The system of claim 5, wherein the validation system further includes a proximity detector causing the communication device to initiate the wireless data communication with the programmable tag upon detecting an object outside the designated area.

9. (Original) The system of claim 1, wherein the communication device is a programmable tag reader exposed outside the designated area to establish a wired data communication with the programmable tag.

10. (Original) The system of claim 1, wherein the validation system includes an input device to enter the second key.

11. (Original) The system of claim 10, wherein the input device is a keypad.

12. (Original) The system of claim 1, wherein the security device is an electronic lock.

13. (Original) The system of claim 1, wherein the security device is a garage door opener.

14. (Original) The system of claim 1, wherein, for each access to the designated area, the programmable unit randomly generates an encryption key to be included in both the first and second keys.

15. (Original) The system of claim 1, wherein the control unit causes the security device to terminate the access to the designated area after a predetermined period of time.

16. (Original) The system of claim 15, wherein the control unit prevents further access to the designated area after the predetermined period of time.

17. (Original) The system of claim 1, wherein the control unit includes a clock to determine the time and date of the access.

18. (Original) The system of claim 17, wherein the control unit stores the time and date of the access in the memory.

19. (Original) The system of claim 17, wherein the communication device transmits to and stores in the programmable tag the time and date of the access.

20. (Original) A method for controlling access to a designated area, the designated area having a security device to control access thereto, comprising the steps of:

generating a first and second key for each access to the designated area;

using the first key, generating an access key;

using the second key, generating a validation key; and

comparing the access key and the validation key and causing the security device to allow access to the designated area if the access key matches the validation key.

21. (Original) The method of claim 20, wherein the first key generating step comprises the steps of:

randomly generating an encryption key; and

combining the encryption key with a third key.

22. (Original) The method of claim 21, wherein the second key generating step comprises the step of combining the encryption key with a fourth key.

23. (Original) The method of claim 22, wherein the third key is the address of the designated area and the fourth key is an agent code.

24. (Original) The method of claim 23, wherein the access key generating step comprises the steps of:

entering the first key, the agent code, the address, and an access date;

comparing the entered address and the address in the first key; and

using the encryption key, encrypting the agent code, the access date, and the address if the entered address matches the address in the first key.

25. (Original) The method of claim 24, wherein the validation key generating step comprises the steps of:

entering the second key, the agent code, the address, and the access date;

comparing the entered agent code and the agent code in the second key; and;

using the encryption key, encrypting the agent code, the access date, and the address if the entered agent code matches the agent code in the second key.

26. (Original) The method of claim 20, further comprising the step of causing the security device to terminate the access to the designated area after a predetermined period of time.

27. (Original) The method of claim 26, further comprising the step of preventing further access to the designated area after the predetermined period of time.

28. (Original) The method of claim 20, further comprising the step of storing the time and date of the access.

Evidence Appendix to Appeal Brief Under Rule 41.37(c)(1)(ix)

None.

Related Proceedings Appendix to Appeal Brief Under Rule 41.37(c)(1)(x)

None.